



PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

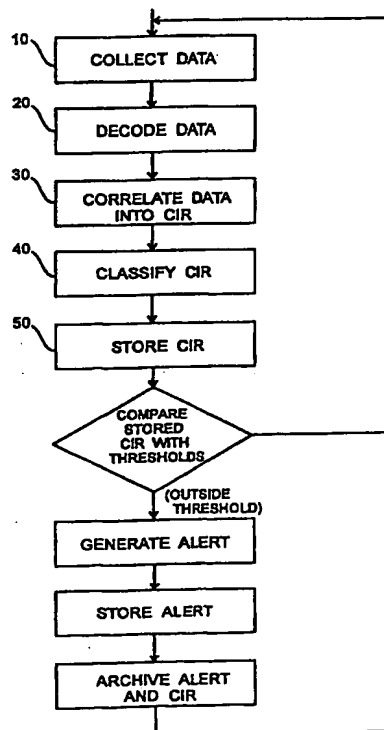
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

| | | | |
|--|--|----|--|
| (51) International Patent Classification ⁶ : H04M 3/00, 7/00, 15/00 | | A1 | (11) International Publication Number: WO 98/39899 (43) International Publication Date: 11 September 1998 (11.09.98) |
| (21) International Application Number: PCT/US98/03507 (22) International Filing Date: 23 February 1998 (23.02.98) (30) Priority Data: 08/807,039 24 February 1997 (24.02.97) US (63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Application US 08/807,039 (CON) Filed on 24 February 1997 (24.02.97) (71) Applicant (for all designated States except US): AMERITECH CORPORATION [US/US]; 2000 West Ameritech Center Drive, Hoffman Estates, IL 60196 (US). (72) Inventors; and (75) Inventors/Applicants (for US only): BETTS, Judy, Lynn [US/US]; 5955 Kilbury-Huber Road, Plain City, OH 43064 (US). HATLAK, Michael, J. [US/US]; 366 Mensching Road, Roselle, IL 60172 (US). McGUIRE, Michael, J. [US/US]; 4308 S. Maple Avenue, Stickney, IL 60402 (US). | | | (74) Agent: HETZ, Joseph, F.; Brinks Hofer Gilson & Lione, NBC Tower, Suite 3600, 455 North Cityfront Plaza Drive, Chicago, IL 60611 (US). (81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG). |
| | | | Published With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments. |

(54) Title: SYSTEM AND METHOD FOR REAL-TIME FRAUD DETECTION WITHIN A TELECOMMUNICATIONS SYSTEM

(57) Abstract

Real-time detection of the fraudulent use of a telecommunications network is accomplished by analyzing data for each call that is occurring within the network. A signal protocol receiver is used to collect signaling protocol (10) for each call that is occurring within the network. The Signaling protocol data is collected, decoded (20) and formatted (30) into call information records (CIRs). The CIRs contain various operator specified parameters (40) for each call that is occurring within the network. The CIRs are compared to operator defined thresholds (60). If any of the CIRs exceeds the thresholds, an alert is generated (70). The alerts are stored (80) in a database so that trends of fraudulent use can be detected and prevented. This method of fraud detection provides for the effective analyzation of every call that is occurring within the network. Accordingly, no call goes unanalyzed and ideally no fraud goes undetected. Additionally, the method does not impose an additional load on the network switching equipment and therefore results in a better quality of transmissions.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|----|--------------------------|----|--|----|--|----|--------------------------|
| AL | Albania | ES | Spain | LS | Lesotho | SI | Slovenia |
| AM | Armenia | FI | Finland | LT | Lithuania | SK | Slovakia |
| AT | Austria | FR | France | LU | Luxembourg | SN | Senegal |
| AU | Australia | GA | Gabon | LV | Latvia | SZ | Swaziland |
| AZ | Azerbaijan | GB | United Kingdom | MC | Monaco | TD | Chad |
| BA | Bosnia and Herzegovina | GE | Georgia | MD | Republic of Moldova | TG | Togo |
| BB | Barbados | GH | Ghana | MG | Madagascar | TJ | Tajikistan |
| BE | Belgium | GN | Guinea | MK | The former Yugoslav Republic of Macedonia | TM | Turkmenistan |
| BF | Burkina Faso | GR | Greece | | | TR | Turkey |
| BG | Bulgaria | HU | Hungary | ML | Mali | TT | Trinidad and Tobago |
| BJ | Benin | IE | Ireland | MN | Mongolia | UA | Ukraine |
| BR | Brazil | IL | Israel | MR | Mauritania | UG | Uganda |
| BY | Belarus | IS | Iceland | MW | Malawi | US | United States of America |
| CA | Canada | IT | Italy | MX | Mexico | UZ | Uzbekistan |
| CF | Central African Republic | JP | Japan | NE | Niger | VN | Viet Nam |
| CG | Congo | KE | Kenya | NL | Netherlands | YU | Yugoslavia |
| CH | Switzerland | KG | Kyrgyzstan | NO | Norway | ZW | Zimbabwe |
| CI | Côte d'Ivoire | KP | Democratic People's Republic of Korea | NZ | New Zealand | | |
| CM | Cameroon | KR | Republic of Korea | PL | Poland | | |
| CN | China | KZ | Kazakhstan | PT | Portugal | | |
| CU | Cuba | LC | Saint Lucia | RO | Romania | | |
| CZ | Czech Republic | LI | Liechtenstein | RU | Russian Federation | | |
| DE | Germany | LK | Sri Lanka | SD | Sudan | | |
| DK | Denmark | LR | Liberia | SE | Sweden | | |
| EE | Estonia | | | SG | Singapore | | |

SYSTEM AND METHOD FOR REAL-TIME FRAUD DETECTION WITHIN A TELECOMMUNICATIONS SYSTEM

TECHNICAL FIELD

This invention relates generally to detecting fraudulent use of a resource such as a telecommunications network and particularly to methods and systems for detecting and analyzing fraudulent use of a telecommunications network in real-time.

BACKGROUND OF THE INVENTION

Modern telecommunications networks consist of a number of interconnected switches which may be provided by a common operating company. Individuals may gain unauthorized access to the network to use the network resources without paying services charges to the operator. Such unauthorized use often results in the wrong party being charged for the use because the fraudulent user is unknown. When the wrong party is charged for the unauthorized use, the telecommunication network's operator will be unable to collect the charges. Such unauthorized use may account for a significant portion of a network operating expenses and impose a financial burden on the operating company.

Fraudulent use of a telecommunications network also consumes valuable network resources which may degrade the quality of service provided to legitimate customers. The misuse of network resources denies legitimate customers access to the network.

An effective way of preventing fraudulent use of a network is to detect the misuse as it occurs. If the misuse is detected as it is occurring, it may then be prevented before or as it occurs. The ability to detect fraudulent use in real-time can thus significantly reduce the financial burden imposed on a network operator. Accordingly, a network which accurately detects fraudulent use of a telecommunications network, in real-time, is needed.

Prior systems have attempted real-time fraud detection. One example of such a system is disclosed in U.S. Patent No. 5,495,521 to Rangachar, which describes a method and means for preventing fraudulent use of a telephone

network. The system described therein utilizes the switching equipment located within a network's central offices to collect data and create a call detail record. The call detail record information is automatically generated by the switching equipment to provide data that is analyzed to detect fraudulent network use.

5 One problem with this data collection technique is that the switching equipment's primary function is to switch traffic within the system. The creation of call detail records, however, is a secondary function of the switching system. Accordingly, the switching equipment is not a efficient mechanism for generating call detail records. Also, the switching equipment is equipped with hardware and
10 extensive software which facilitate the switching of calls. The software may include upgrades and patches which can interfere with the switching and cause the switch to malfunction. This combination of shortcomings results in a data collection method where a call detail record may not be created for all calls. Accordingly, some fraudulent calls may go undetected.

15 Another problem with prior data collection methods is that the call records are dependent upon the individual switches. Typically, the call record format is determined by the particular switch handling the call. A network may contain a number of different types of switches. Each switch is programmed to create a call detail record which includes predetermined parameters. Thus, the modification of
20 call detail records generated at the switch level requires the modification of all switches within the telecommunications network that is being monitored for fraud.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic view of a real-time fraud detection system for use in a
25 modern telecommunications network.

FIG. 2 is a flow chart describing the process of using the system of FIG. 1 to perform real-time fraud detection within a modern telecommunications network.

FIG. 3 is a graphic representation of a call information record.

30

DETAILED DESCRIPTION OF THE PRESENTLY PREFERRED
EMBODIMENTS

The preferred embodiment of the present invention enables a
5 telecommunications network operator to detect fraudulent use of a
telecommunications network in real-time. The fraud detection is accomplished by
effectively analyzing data associated with each call placed through the
telecommunications network. The preferred embodiment of the invention enables
the operator to analyze a customizable set of call information records in order to
10 detect fraudulent calls. The customizable set of call information records is
modifiable or customizable independent of the switching equipment within the
network. The preferred embodiment also allows for the detection of fraud in a
manner which does not load the switching equipment within a network, thereby,
resulting in a better quality of service within the network.

15 Referring now to FIGS. 1 and 3, the preferred embodiment of the invention
incorporates a real-time fraud detection system 20 into a modern
telecommunications network 10. Modern telecommunications networks typically
utilize a signaling protocol 22 to control the switching of voice and data traffic
within the network 10. Many different types of existing signaling protocols may be
20 utilized. These signaling protocols may take two common forms, in-band signaling
and out-of-band signaling. In-band signaling protocols are interspersed with the
voice and data transmissions that are carried over the network. In-band signaling
protocols are transmitted with voice and data transmissions between common
elements within the network 10. Thus, the in-band signaling protocols are
25 transmitted between the same switches which carry the voice and data
communications over the network 10. For example, one such type of in-band
signaling protocol is Multiple Frequency R1 (MFR1).

In comparison to in-band signaling, out-of-band signaling protocols are
segregated from the corresponding voice and data transmissions. Out-of-band
30 signaling protocols are transmitted along different transmission channels than those
that carry voice and data transmissions. Typically, out-of-band signaling protocols
are transmitted between the central offices 30 and signal transfer points (STPs) 36.

For example, Signaling System 7 (SS7) is one such type of out-of-band signaling protocol.

The present embodiment includes a signal protocol receiver 40 for collecting signaling protocols 22 transmitted within the telecommunications network 10. The collection of network signaling protocol transmissions is well known to those skilled in the art. The signal protocol receiver 40 is separate from the switching equipment within the central offices 30 and the STPs 36 in the network 10. The signal protocol receiver 40 collects the signaling protocol transmissions 22 and does not handle call switching. The signal protocol receiver 40 allows for the non-intrusive monitoring of calls occurring within the network 10.

The present embodiment utilizes the signal protocol receiver 40 to detect fraudulent calls within networks that utilize either in-band signaling protocols or out-of-band signaling protocols. The signal protocol receiver 40 collects signaling protocols 22 associated with each call placed through the network 10. One problem with in-band signaling protocols is that a centralized point of collection does not exist. Thus, to capture in-band signaling protocols, a signal protocol receiver 40 must be located at each switch 32 within the central offices 30 of the network 10. The signal protocol receiver 40 collects the data by sampling the transmitted signaling protocols 22 from the switching equipment 32 in the central offices 30 of the network 10.

Out-of-band signaling protocols have a centralized point of collection as all transmissions are sent through STPs 36. Thus, to capture out-of-band signaling protocols, a signal protocol receiver 40 is located at each STP 36 within the network 10. The signal protocol receiver 40 collects data associated with all of the calls occurring within the network 10. The signal protocol receiver 40 collects the data by sampling the signaling protocol transmissions transmitted via the STPs 36.

With both out-of-band and in-band signaling formats, the signal protocol receiver 40 collects call data directly from the ongoing transmission by using a high impedance bridge tap well known to those skilled in the art. The bridge tap allows for the effective collection of data without affecting the quality of transmissions with the network 10. By utilizing a dedicated signal protocol receiver 40, which is

independent from the switching equipment in the central offices 30 and the STPs 36, to collect signaling protocols 22, call data can be effectively collected for every call through the network 10. Accordingly, calls are not missed, and each fraudulent call can be detected. Also, the signal protocol receiver 40 does not
5 produce a load on the switches in the central offices 30 or the STPs 36, which handle the switching of signaling protocols and voice and data transmissions. The independent signal protocol receiver 40 removes the burden of creating call records from the switching equipment in the central offices 30 and the STPs 36, allowing for better quality transmissions.

10 After the signaling protocol data 22 is collected, it is decoded into a useable format. A decoder 42 is used to decode the data as it is collected. For example, decoder 42 transforms the signaling protocol transmissions 22 into a call parameter data 24 which can be analyzed. The decoder 42 formats the transmitted signaling protocol transmissions into call information records 26 (CIRs) using
15 standard high level programming data structures. The CIRs 26 can include various parameters associated with an ongoing call. Some commonly used parameters include: originating; terminating; billing type; using duration; aggregate duration; call volume; etc. The selective incorporation of parameters included in the CIRs 26, eliminates unnecessary data, allowing the signaling protocol data 22 to be
20 processed in a more efficient manner. It also enables the operator to adapt the fraud system 20 to changing requirements by adding new parameters to the CIRs 26 as such parameters become key indicators of fraudulent calls.

In a preferred embodiment, the signal protocol receiver 40 collects and decodes the signaling protocol data into a CIR 26. The signal protocol receiver 40
25 can programmed to create various types of CIRs 26 based upon the operator's preferences. An operator can choose the specific call parameters that are included within a CIR 26. The signal protocol receiver 40 can then be programmed to create CIRs 26 which incorporate the specific combination of parameters chosen by the operator. Thus, the system can be modified by programming the signal
30 protocol receivers 40 within the network 10. Accordingly, the system is modifiable independent from the switching equipment within the central offices 30 and the

STPs 36. A common signal protocol receiver/decoder is the call completion analysis system manufactured by Tekno Industries of Bensenville, Illinois.

After the signaling protocols 22 have been collected and decoded, the resulting CIRs 26 are analyzed to determine if unauthorized use of the network 10 is occurring. The CIRs 26 are transmitted from the decoder 42 to a pre-processor 44. The pre-processor 44 classifies the CIRs 26 based upon the CIR 26 parameters. The pre-processor 44 classifies the CIRs 26 into three basic categories: originating; terminating; and bill to type. Within each basic category, the pre-processor 44 further classifies the CIRs 26 into sub-categories such as national, cellular, international, pay phone hot numbers, etc. The classification is configurable and modifiable. This configurability allows the operator to change the monitoring and classification process as different techniques for detecting fraud are developed. The pre-processor 44 also has the ability to discard undesirable CIRs 26 and count the number of CIRs 26 that are discarded. For example, one type of an undesirable CIR 26 may be a duplicate record. In a preferred embodiment, the functionality of the pre-processor 44 is implemented with an NT computer operating system platform. The NT operating system platform allows for an inexpensive modular format which allows the system to be easily expanded or modified as new techniques for detecting fraud are developed. Additionally, the preferred embodiment may be implemented with software as known to those of skill in the art. For example, the preferred embodiment may be written in a high level programming language such as Pascal, C or C++.

After the CIRs 26 are classified, they are analyzed to determine whether unauthorized use is occurring. The CIRs 26 are transmitted from the pre-processor 44 to a watch point processor 46. The watch point processor 46 stores CIRs 26 in a random access memory or a data base 48. Once the CIRs 26 are stored, the watch point processor 46 can continuously apply control techniques to the CIRs 26 in the database 48. The control techniques enable the operator to monitor the various parameters of the CIRs 26 in an organized manner. Some call parameters which can be monitored include: duration, aggregate duration, volume, volume/duration, and simultaneous calls. The control techniques allow for a number of thresholds 60 to be applied to the CIRs 26. The control technique

compares the operator defined thresholds 60 to selected parameters of the CIRs 26. When any of the thresholds 60 is satisfied or exceeded, an alert 62 is generated. The thresholds 60 can be applied to a singular CIR 26 and/or groups of CIRs 26. The CIRs 26 can also be compared to one another on a singular or a group basis in order to detect fraud. This methodology allows for a very diverse range of threshold analysis in an attempt to detect fraudulent use which occurs in a variety of forms, as the fraudulent use is occurring. One example of CIR data that may indicate fraudulent use is multiple successive calls charged to the same customer. Another such example is calls with long durations charged to a common customer.

Preferably, the watch point processor 46 and its accompanying control technique software utilizes a UNIX operating system based platform. The development of the control technique software is well understood by those skilled in the art. The UNIX-based system allows for the scalability needed to monitor data from a very small number of switches to hundreds of switches simultaneously. Additionally, the preferred embodiment may be implemented with software as known to those of skill in the art. For example, the preferred embodiment may be written in a high level programming language such as Pascal, C or C++.

The alerts 62 generated by the watch point processor 46 are utilized to signal the operator that fraud has been detected. The alerts 62 generated can be in the form of audible, visual, or a remote alert. A audible or visual alert can be generated by the fraud system 20 to alert the operator that fraud has been detected. Additionally, a remote alert 62 can be sent to an operator via a cellular telephone or a pager system. After receiving the alert 62, the operator may analyze the alerts and take the proper action in response. The operator can notify the customer whose resources are being fraudulently used or the operator can suspend the fraudulent use by cutting off the user and denying further access to the network 10. In addition to notifying the operator that fraud is occurring, the alerts 62 can be analyzed to detect patterns of fraud. According to a preferred embodiment, when an alert 62 is generated by the watch point processor 46 it is sent to the fraud analysis processor 50. The fraud analysis processor 50 stores each alert 62 in a random access memory or a database 52.

In addition to storing the alerts 62, the fraud analysis processor 50 receives all the CIRs 26 to create a database 54 containing every call that occurs within the network 10. The archiving of information enables a telecommunications network operator to analyze the most recent alerts 62 and CIRs 26 to detect patterns or trends of fraud that are occurring. In a preferred embodiment, the CIRs 26 are stored eight days for customer profiling and daily alert generation. The CIR 26 data is stored in daily tables and indexed according to type of call such as international, domestic, high risk areas, toll free, etc. This data is analyzed daily to detect unusual patterns such as increased traffic volume by number of attempts or duration. For example, the fraud analysis processor 50 compares today's traffic for each unique number to the previous days data and the same day last week. Changes in traffic patterns such as short-term or duration increases in traffic volume can be highlighted. This method detects subscribers that have had their services compromised or even subscribers that are new and are running up large call volumes. The fraud analysis processor 50 allows the operator to detect fraudulent calls early so the operator can take a pro-active measures. For example, new high risk customers that have large volumes within the first week of service may be required to supply deposits to continue service. Additionally, the preferred embodiment may be implemented with computer software as known to those of skill in the art. For example, the preferred embodiment may be written in a high level programming language such as Pascal, C or C++.

In the presently preferred embodiment, the steps of establishing thresholds 60 and generating and analyzing alerts 62 can be enhanced by utilizing a graphic user interface (GUI). The graphic user interface includes all the graphical tools needed to setup and display the pre described functions. Each system element may have its own integrated GUI. For example, the signal protocol receiver/decoder 40 has a GUI that allows the operator to define the CIRs easily and efficiently. The pre-processor 44 has a GUI that displays the status of all call parameters as well as the setup and configuration of the pre-processor 44. The watch point processor 46 has a GUI that allows the operator to setup the thresholds easily and efficiently. The fraud analysis processor 50 has a GUI that allows the operator to analyze the alerts 62, take appropriate action to resolve the alerts 62 and commit all activity

into a fraud log . Preferably, all the GUI interfaces are integrated onto one platform, a NT computer operating system based work station. Additionally, the preferred embodiment may be implemented with software well known to those of skill in the art. For example, the preferred embodiment may be written in a high level programming language such as Pascal, C or C++. The interface is constructed in such a way that any number of operators can access the CIR data and analyze the alerts. The result is an integrated solution for combating fraudulent activity in the telecommunications network 10 in a real-time/in-progress manner.

Referring now to FIG. 2, the system described above is utilized to perform real-time fraud detection. Real-time call data is collected for each call that is occurring through a telecommunications network. The signal protocol receiver (FIG. 1) collects signaling protocol data directly from the transmissions of the data. The signal protocol receiver is capable of collecting both in-band signaling protocol data and out-of-band signaling protocol data, as described in detail above. After the signaling protocol data is collected it is decoded and transformed to a useable format. A decoder (FIG. 1) is used to decode the signaling protocol data. The decoder can decode signaling protocol data that is extracted from a network using either in-band or out-of-band signaling protocols. The decoder transforms the data into a useable form. After the data is decoded, it is correlated into a call information record (CIR). The decoder formats the decoded data into a CIR that contains various call parameters and is created according to predetermined operator preferences.

After the CIRs are created, they are analyzed to determine whether fraudulent calls are occurring. The CIRs are transmitted to a pre-processor which classifies the CIRs, as described above. The pre-processor classification eliminates unneeded portions of the data that is collected. After the CIRs have been classified, they are transmitted to the watch point processor (FIG. 1). The watch point processor stores the CIRs in a random access memory. The stored CIRs are compared to predetermined operator defined thresholds by the watch point processor. If any of the CIRs are not within the thresholds, an alert is

generated 70 by the watch point processor. The alerts can be in the form of audible, visual or remote, as described in detail above.

5 The alerts are transmitted to the fraud analysis processor (FIG. 1) where they are stored 80 in a random access memory. The storage of the alerts enables a operator to analyze the alerts and take the appropriate action to terminate the fraudulent call or transmission. The alerts and CIRs are also archived 90 by the fraud analysis processor (FIG. 1). This archival of data facilitates the analyzation of data to determine trends of fraud. All of the steps described above can be accomplished in real time during the duration of the call.

10 It is to be understood that the steps of pre-processing, watch point processing and fraud analysis processing could be accomplished by utilizing a single processor equipped with the necessary peripherals. Accordingly, all of the storage and archival steps could be accomplished by utilizing a single database.

The current embodiment of the present invention provides an improved
15 method and system for detecting fraudulent use of a telecommunications network. The embodiment enables the detection of fraud by effectively analyzing the signaling communication protocol transmissions that are associated with each existing call. The embodiment enables the operator to analyze a customized set of call detail records by selecting which call parameters will be incorporated into the
20 call detail records. By collecting data directly from a STP, the embodiment allows for the detection of fraud in a manner which places no additional load on the switching equipment which handles the voice and data transmissions within a network.

It is also to be understood that a wide range of changes and modifications
25 to the embodiments described above will be apparent to those skilled in the art and are contemplated. It is therefore intended that the foregoing detailed description be regarded as illustrative rather than limiting, and that it be understood that it is the following claims, including all equivalents, that are intended to define the spirit and scope of the invention.

We claim:

1. A method for detecting fraudulent access to a telecommunications network comprising the steps of:
providing a signal protocol receiver independent from a network switching
5 equipment;
collecting signaling protocol data for a call from the telecommunications network using the signal protocol receiver;
decoding the signaling protocol data;
correlating the signaling protocol data into call information records;
10 analyzing the call information records during the duration of the call to detect fraudulent use of the telecommunications network.
2. The method of claim 1 further comprising the step of classifying the call information records.
15
3. The method of claim 1 further comprising the step of storing the call information records in a database.
4. The method of claim 1 wherein the step of analyzing the call
20 information records comprises comparing the call information records to pre-established thresholds.
5. The method of claim 1 wherein the step of analyzing the call information records comprise comparing the call information records to one
25 another.
6. The method of claim 4 wherein the step of analyzing the call information records comprises generating an alert when at least one of the call information records exceeds the thresholds.
30
7. The method of claim 6 wherein the alert is in the form of audio, visual or remote.

8. The method of claim 4 wherein the step of analyzing the call information records comprises storing the alerts and call information records in a database and maintaining data for a predetermined number of days, to facilitate an analysis of fraudulent trends.

9. The method of claim 1 wherein the signaling protocol data is in-band and is collected at the switches within a network.

10. The method of claim 1 wherein the signaling protocol data is out-of-band and is collected from the STPs within a network.

11. The method of claim 1 wherein the call information records contain at least one of the following parameters: originating, terminating, billing type, using duration, aggregate duration, call volume.

12. A system for detecting fraudulent access to a telecommunications network comprising:

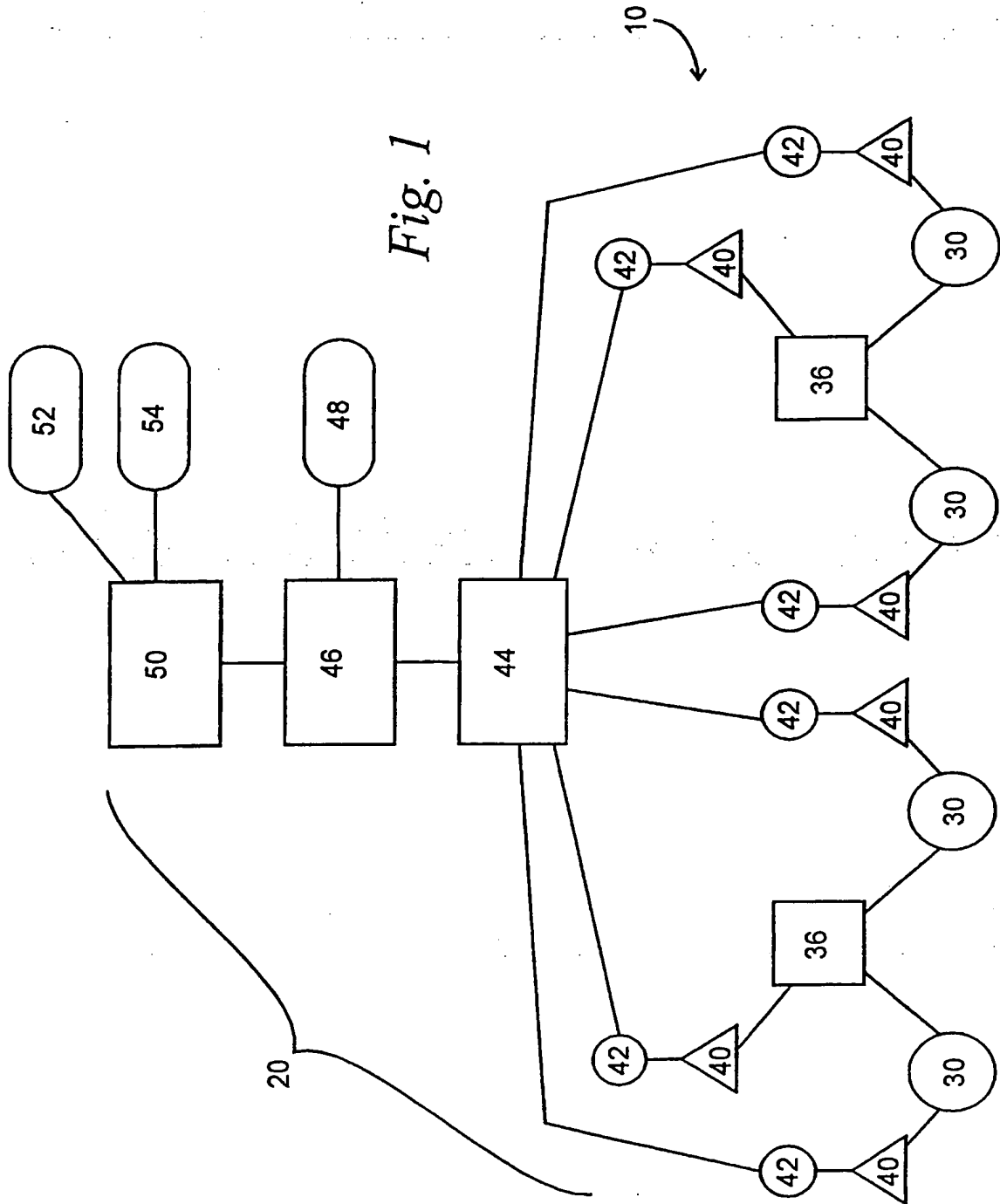
a signal protocol receiver independent from the network switching equipment for collecting signaling protocol data;
a decoder for decoding the signaling protocol data and formulating call information records;
a processor for analyzing the call information records in order to detect fraudulent use of the telecommunications network.

13. The system of claim 12 wherein the processor comprises pre-processor for classifying the call information records and a watch point processor for comparing the call information records to operator defined thresholds

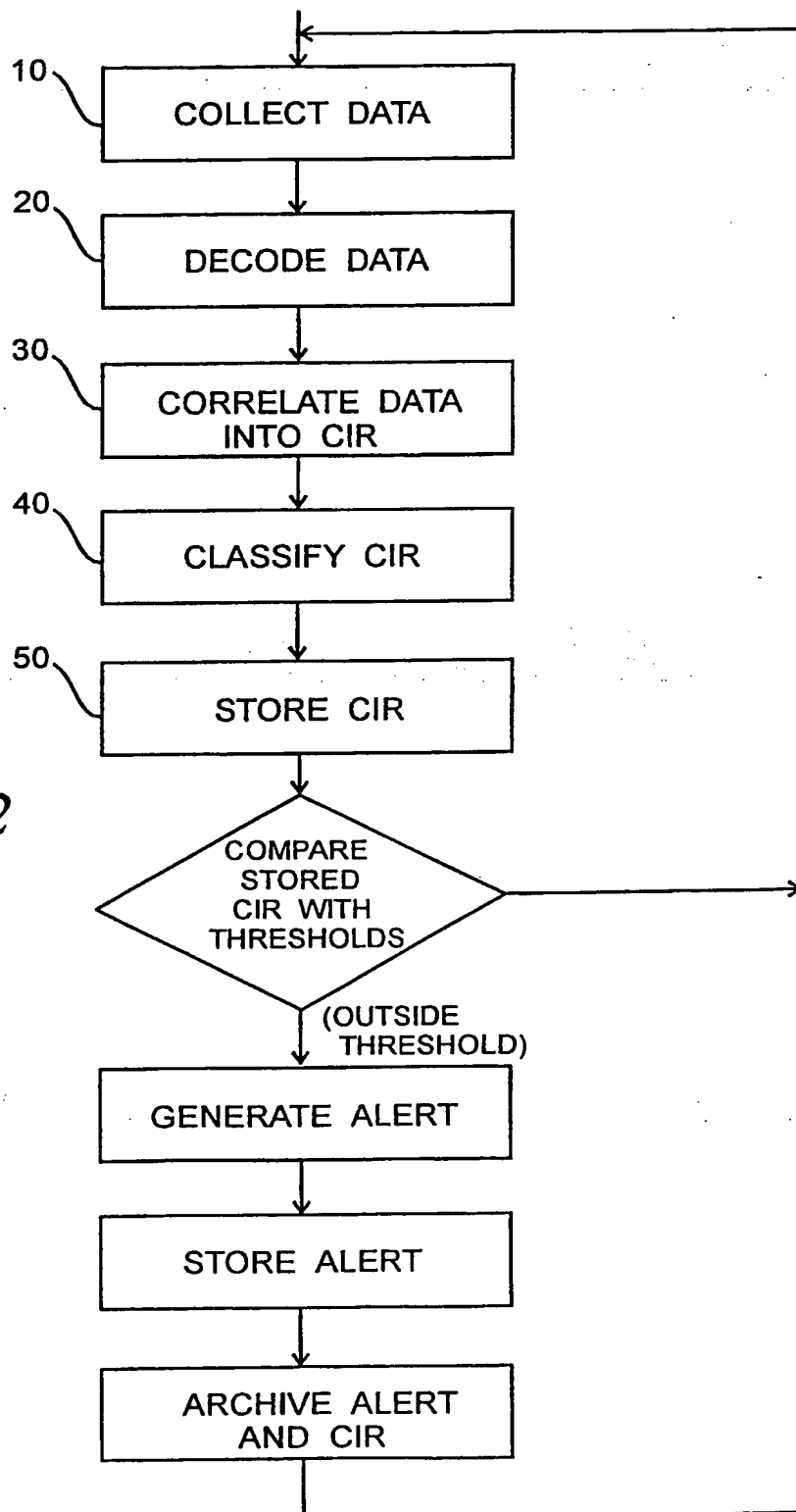
14. The system of claim 12 wherein the processor further comprises a fraud analysis processor for storing the alerts and the call information records in a database.

15. A method for detecting fraudulent access to a telecommunications network comprising the steps of:
- providing a signal protocol receiver independent from the network
 - 5 switching equipment;
 - collecting signaling protocol data from the network using the signal protocol receiver;
 - decoding the signaling protocol data;
 - correlating the signaling protocol data into call information records
 - 10 containing at least one call parameter;
 - classifying the call information records based upon the at least one call parameter;
 - analyzing the call information records by comparing them to pre-established thresholds or other call information records;
 - 15 generating an alert if the call information records exceed the thresholds;
 - storing the alerts in a database;
 - storing the call information recording in a database.

Fig. 1



2/3

*Fig. 2*

26 (CIR)

| | |
|---------------|-------|
| ORIGINATING: | _____ |
| TERMINATING: | _____ |
| BILLING TYPE: | _____ |

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/03507

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04M 3/00, 7/00, 15/00

US CL :Please See Extra Sheet.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 379/189, 188, 111, 219

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|---|-----------------------|
| X,P | US 5,627,886 A (BOWMAN) 06 May 1997, col. 2, lines 1-67, col. 8, lines 11-62, col. 10, lines 48-52. | 1-15 |

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

A document defining the general state of the art which is not considered to be of particular relevance

B earlier document published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

Z document member of the same patent family

Date of the actual completion of the international search

17 JUNE 1998

Date of mailing of the international search report

14 AUG 1998

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

KRISTA ZELE

Telephone No. (703) 305-4701

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/03507

A. CLASSIFICATION OF SUBJECT MATTER:

US CL :

379/189, 188, 111, 219

B. FIELDS SEARCHED

Electronic data bases consulted (Name of data base and where practicable terms used):

APS

search terms: detect?, fraud?, signaling protocol, call information records, threshold, database, compar?, alert, signal transfer points or STPs